4Ш

УДК 004.415.24

И.В. Швидченко
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев
sh_inet@rambler.ru

Стойкие криптостеганографические алгоритмы

В статье предложен подход к улучшению стеганостойкости алгоритмов скрытия информации за счет совместного использования криптографических преобразований информации со стеганографическими. Дана оценка качества криптостеганографических систем.

Введение

Круг задач, решаемых в области защиты информации, постоянно расширяется. Растут требования к качеству их решения. Среди всего спектра методов обеспечения защиты информации в информационных системах особое место занимают криптографические методы защиты информации. В основе последних лежит понятие криптографического преобразования информации, производимого по определенным математическим законам, с целью исключить доступ к данной информации посторонних пользователей, а также с целью обеспечения целостности информации. В современных условиях методы традиционной криптографии в целом ряде задач становятся недостаточными, поскольку не позволяют сохранить в тайне сам факт передачи и/или хранения информации, ее объем и источник. С созданием глобальных телекоммуникационных сетей и образованием цифровой информационной среды подобные проблемы стало возможным решать методами компьютерной стеганографии, позволяющими скрытно внедрять дополнительную информацию в компьютерные данные, представляющие собой различные файлы, программы, пакеты протоколов.

Стеганографические системы

Компьютерная стеганография – активно развивающееся направление в области информационной безопасности. Для решения стеганографических задач применяются известные и разрабатываются новые методы.

Стеганографические методы позволяют эффективно решать следующие задачи:

– сокрытие самого факта передачи и/или хранения конфиденциальной информации;
– защита авторских прав на некоторые виды интеллектуальной собственности в телекоммуникационных сетях («водяные знаки»);
– защита информационных сетей от несанкционированного мониторинга и вмешательства в управление их ресурсами;
– камуфлирование программного обеспечения систем;
– борьба с некоторыми видами компьютерных вирусов («логические бомбы», автономные репликативные программы);
– реализация объемного цифрового телевидения с использованием обычных (не стерео) каналов цифрового телевидения и многие другие задачи [1].

Эффективное решение этих задач позволяет говорить о реальной возможности и целесообразности разработки стеганографических систем, которые могут повысить эффективность решения проблем защиты информации в сфере банковской деятельности и электронной коммерции, в информационных системах военного назначения и т.д.

Преимущество стеганографической защиты состоит в том, что она дает возможность скрытно передавать закрытую информацию одновременно с открытой (видимой) информацией, не имеющей конфиденциального характера. При этом появляется возможность избежать прямых атак на закрытую информацию, поскольку неизвестно, присутствует ли она в информационном потоке, и если да, то что является ее числовым носителем.

В качестве открытой информации могут использоваться, например, оцифрованные изображения (цифровые фотографии, кадры видео-, цифрового телевидения и т.п.). Сокрытие, по сути, сводится к синтезу двух новых числовых носителей (соответственно открытой и закрытой) информации, аналитический вид и параметры которых позволяют образовывать их композицию, по формату совпадающую с открытым (видимым) изображением и сохраняющую неизменным зрительное восприятие синтезированного таким образом заново видимого изображения.

Стеганографические системы могут быть предназначены для достижения различных целей, в зависимости от которых задачи по преобразованию информации в них могут принципиально отличаться как по постановке, так и по методам решения. Одной из главных среди них является максимизация объема скрытно внедряемой информации при обеспечении стойкости изображения-контейнера к визуальному анализу и стеганоанализу с применением программных средств, проводимых с целью выявления факта наличия в нем дополнительной скрытой информации (сообщения).

Анализ известных подходов к построению стеганопреобразований, решающих указанную задачу, показывает, что наиболее перспективным направлением (с точки зрения возможности выполнения основного требования – стойкости к обнаружению факта скрытого внедрения сообщения) является разработка стеганопреобразований на основе использования так называемой «визуальной избыточности», присущей цифровым описаниям изображений в стандартных форматах. Визуальная избыточность, являющаяся следствием психофизиологических особенностей восприятия изображения человеком, позволяет при полном соблюдении правил построения файлов, не создавая легко обнаруживаемых признаков внедрения сообщения (не занимая присущие формату «пустоты» в файле, не подменяя второстепенную служебную информацию, не искажая стандартные описания цветовой палитры и т.п.), передавать значительный объем конфиденциальной информации, изменяя в определенной степени непосредственно цифровое описание изображения, внешне не проявляя своего существования и сохраняя неизменным его зрительное восприятие.

В настоящее время на рынке программных продуктов можно встретить достаточное количество стеганопрограмм, разработанных под некоторые форматы графических, видео- и аудиофайлов, используемых в Интернете. В большинстве из них применяются различные модификации LSB-метода – использование нескольких младших двоичных разрядов интенсивности цветовых компонент отдельных пикселей. Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации. В то же время недостатком такого подхода является слабая устойчивость заполненного контейнера к атакам, проводимым с целью обнаружения факта существования в нем скрытой информации [2]. К тому же стеганографические преобразования, использующие метод наименее значимых бит, обладают высокой чувствительностью к малейшим искажениям контейнера.

Более стойкими к разнообразным искажениям считаются методы, использующие для скрытия данных не пространственную область контейнера, а спектральную. Среди большинства программ, работающих со спектром контейнера, используют для сокрытия коэффициенты дискретного косинусного преобразования (ДКП) или вейвлет-преобразования (ВП). Однако использование ДКП и ВП в компьютерной стеганографии дает каналы, обладающие небольшой пропускной способностью, поэтому они в первую очередь используются для защиты авторских прав, внедряя в контейнер оригинальный цифровой водяной знак небольшого размера. Для сокрытия максимально большого объема данных при обеспечении стойкости контейнера к атакам пассивного и активного противника можно использовать преобразование Фурье (ПФ). На основе ПФ разработан программный комплекс, который выполняет стеганографическое скрытие информации с помощью алгоритма, реализованного на базе теоремы про свертку [3]. Пропускная способность стеганоканала данного метода соизмерима с пропускной способностью метода НЗБ.

В общем случае любая стеганографическая система представлена в виде совокупности объектов $S=(C,M,K,Q,H,R)$, где C и Q – множества пустых и заполненных контейнеров, M – множество скрываемых сообщений, $K=\{0,1,..n-1\}$ – множество ключей, $H=\{h_k,k\in K\}$ – множество правил внедрения сообщений из $m\in M$ в контейнеры $c\in C$, $R=\{r_k,k\in K\}$ – множество соответствующих элементам из $h_r\in H$ правил восстановления (извлечения) сообщений из контейнеров $q\in Q$. В реальных системах сложность перестройки алгоритмов внедрения сообщений в зависимости от ключа привела к тому, что в большинстве решений стеганографические ключи не используются. В тех же случаях, когда в программном продукте предлагается использование дополнительных ключей, в действительности оказывается, что эти ключи не являются ключами встраивания, а представляют собой ключи используемых в неявном виде шифров. Зачастую ими оказываются тривиальные шифры перестановки и подстановки. В обоих случаях стеганографическая система представима в виде $S=(C,M,Q,h,r)$, где h,r – не зависящие от ключа, бесключевые правила внедрения и извлечения информации. Построение реальных ключевых стегосистем является достаточно сложной задачей, требующей разработки легко перестраиваемых алгоритмов сокрытия информации, что в большинстве случаев либо нерационально, либо просто невозможно в связи с предъявляемыми требованиями к уровню скрытности и ограничениями на полосу передачи данных. Поэтому возникает вопрос о возможности построения стойких стеганографических систем на основе систем $S=(C,M,Q,h,r)$ с определенным, приемлемым уровнем стойкости к обнаружению.

Подход к построению стойких стеганографических систем

Поскольку принято считать, что стеганосистема $S=(C,M,Q,h,r)$ должна обеспечивать защиту сообщения при условии, что стеганоалгоритм полностью известен потенциальному противнику (согласно второму правилу Керкгоффса), то надежность скрытия факта внедрения сообщения и его неизвлекаемость должны обеспечиваться организацией в стеганосистеме специальной «внутренней» (т.е. органически входящей в ее структуру) криптозащиты с использованием секретного ключа. Алгоритм

внутренней криптозащиты требуемого качества может быть создан на базе теоретически обоснованных методов шифрования в соответствии с действующим законодательством конкретной страны, государственным статусом пользователя стеганосистемы, объявленными им целями применения стеганосистемы и требуемой эффективностью внутренней криптозащиты системы.

Большинство существующих стеганографических алгоритмов оперируют входными данными вне зависимости от их статистических характеристик. В действительности же распределение входных данных для стеганографических алгоритмов играет очень важную роль. В общем случае, для того чтобы стеганографическая система обладала высокой стойкостью к атакам пассивного противника, необходимо выполнение следующих условий:

1. Должна сохраняться функциональность контейнеров. Заполненный контейнер должен обладать свойством естественности, т.е. принадлежать множеству всех возможных контейнеров $Q \subseteq C$.

2. Распределение $P(C \cup Q)$ должно быть равномерным, т.е.

$$\forall c \in C \cup Q : p(c) = 1/|C \cup Q| = 1/|C| .$$

3. В процессе записи информации в контейнер должны сохраняться все статистические характеристики любого из распределений полученных в результате вычисления всех возможных функций $f : Q \to X$, где X – некоторое произвольное множество.

4. Для любого контейнера $c \in C \cup Q$ вероятность того, что в нем содержится дополнительная информация, должна быть равна 1 (пустой контейнер тоже содержит в себе информацию).

5. Внедрение информации в контейнер должно осуществляться не за счет записи в него дополнительной информации, а за счет изменения уже существующей $\forall m \in M, c \in C : H(q) = H(c), q = h(m,c)$.

Из требований 3 – 5 можно сформулировать дополнительные требования, касающиеся элементов $m \in M$. Распределение возможных сообщений $m \in M$ должно быть равномерным, а распределение элементов отдельного сообщения m должно соответствовать распределению той информации в контейнере, которая будет замещена в процессе записи сообщения m в контейнер.

Можно заметить, что производные требования к элементам множества M соответствуют требованиям, сформулированным К. Шенноном для совершенных шифров. Таким образом, для того, чтобы стеганосистема обладала высоким уровнем стойкости, применяемые в ней стеганографические алгоритмы должны максимально полно отвечать представленным выше требованиям, а предварительная обработка скрываемых сообщений – включать в себя этап шифрования передаваемых сообщений. Этап шифрования в данном случае позволит, во-первых, обезопасить информацию пользователя от раскрытия ее содержания в случае извлечения сообщения, во-вторых, изменить статистические характеристики сообщения, достичь равномерности распределения секретного сообщения по контейнеру. И что наиболее важно, именно шифрование не позволяет противнику однозначно установить факт передачи информации. Заметим, что из любого контейнера противник может извлечь некоторое сообщение. В случае, если характеристики сообщений, извлеченных из пустого и заполненного контейнеров, совпадут, без знания самого передаваемого сообщения или какой-либо другой дополнительной информации, однозначно, установить факт скрытой передачи

сообщения будет невозможно. Таким образом, ключ шифрования может быть использован в качестве ключа стеганографической системы. Саму стеганографическую систему в данном случае будем называть криптостеганографической. В общем случае такая система обладает стойкостью, эквивалентной стойкости используемых в ней алгоритмов шифрования, но только тогда, когда применяемые стеганографические алгоритмы отвечают описанным выше требованиям [4].

Контроль качества криптостеганографических систем

Задача оценки контроля искажений (контроль качества) растровых графических изображений, вносимых стеганографическими системами, является одной из основных задач стеганографического анализа. Методы контроля искажений позволяют дать количественную оценку изменениям, произошедшим в результате внедрения конкретного сообщения в конкретный контейнер, т.е. найти компромисс между величиной искажений, характеризующей стойкость стеганографической системы как к атакам активного, так и к атакам пассивного противника, и пропускной способностью канала скрытной передачи.

Критерий оценки качества растровых графических изображений – это метрика между исходным (неискаженным, обозначим его C) и модифицированным (искаженным, обозначим его S) растровым графическим изображением. Понятие качества определяется как мера восприятия человеком вносимых искажений в исходное изображение [5].

В ходе данной работы получена оценка качества стеганографических систем, построенных на методе наименее значимых бит и методе преобразования Фурье. Тестировались разные изображения, менялось количество вносимой информации. Приведем результаты одного из исследований.

Рассматривался пустой сигнал-контейнер, который разбивался на блоки 8×8 пикселей. Сообщение, в виде текстового файла, в случае сокрытия в дискретной свертке сигналов занимало максимально возможную для выбранного контейнера длину, в случае НЗБ – 1/3 контейнера. Для скрытия сообщения методом НЗБ использовался программный модуль, реализованный в системе MathCAD [6]. Перед внедрением сообщение шифровалось.

В качестве внутренней криптозащиты брался алгоритм Advanced Encryption Standard (AES), также известный как Rijndael, разработанный двумя криптографами из Бельгии, Винсентом Риджменом (Vincent Rijmen) и Джоаном Дайменом (Joan Daemen) в 2000 году. Алгоритм представляет собой симметричный блочный шифр, который имеет ряд преимуществ: высокую скорость шифрования, минимальные требования к вычислительным ресурсам, стойкость к подавляющему большинству атак по времени выполнения и потребляемой мощности и возможность использования любых комбинаций размеров блока и длин ключа, которые кратны 32 бит. Стойкость Rijndael к дифференциальному и линейному методам криптоанализа эквивалентна сложности простого перебора ключей. Алгоритм не защищен патентами и доступен для свободного использования в любых продуктах. Для шифрования была выбрана реализация алгоритма с длиной ключа и блока 128 бит.

В табл. 1 представлен ряд показателей, используемых во время оценки искажений, вносимых стеганографическими преобразованиями в изображение. Отметим, поскольку система, реализованная на базе теоремы про свертку, оперирует в базисе действительных чисел, необходимо учитывать погрешность округления.

Таблица 1 – Показатели визуального искажения

Название показателя искажения	Оригинал	LSB	DFT
Максимальная разность $MD = \max\limits_{x,y} \left\| C_{x,y} - S_{x,y} \right\|$	0	1	0,0823
Средняя абсолютная разность $AD = \frac{1}{XY} \sum\limits_{x,y} \left\| C_{x,y} - S_{x,y} \right\|$	0	0,4992	0,3097
Нормированная средняя абсолютная разность $NAD = \frac{\sum\limits_{x,y} \left\| C_{x,y} - S_{x,y} \right\|}{\sum\limits_{x,y} \left\| C_{x,y} \right\|}$	0	3,4932*10^{-3}	2,167*10^{-3}
Среднеквадратическая ошибка $MSE = \frac{1}{XY} \sum\limits_{x,y} \left(C_{x,y} - S_{x,y} \right)^2$	0	0,4992	0,1211
Нормированная среднеквадратическая ошибка $NMSE = \frac{\sum\limits_{x,y} \left(C_{x,y} - S_{x,y} \right)^2}{\sum\limits_{x,y} \left(C_{x,y} \right)^2}$	0	2,1816*10^{-5}	5,2933*10^{-6}
Отношение «сигнал/шум» $SNR = \frac{\sum\limits_{x,y} \left(C_{x,y} \right)^2}{\sum\limits_{x,y} \left(C_{x,y} - S_{x,y} \right)^2}$	∞	4,5837*10^{4}	1,8892*10^{5}
Максимальное отношение «сигнал/шум» $PSNR = XY \cdot \frac{\max\limits_{x,y} \left(C_{x,y} \right)^2}{\sum\limits_{x,y} \left(C_{x,y} - S_{x,y} \right)^2}$	∞	1,0089*10^{6}	4,1583*10^{6}
L_2-норма $L_2 = \left(\frac{1}{XY} \sum\limits_{x,y} \left\| C_{x,y} - S_{x,y} \right\|^2 \right)^{1/2}$	0	0,7066	0,348
Качество изображения $IF = 1 - \sum\limits_{x,y} \left(C_{x,y} - S_{x,y} \right)^2 \Big/ \sum\limits_{x,y} \left(C_{x,y} \right)^2$	1	0,999978	0,999995
Нормированная взаимная корреляция $NC = \sum\limits_{x,y} C_{x,y} \cdot S_{x,y} \Big/ \sum\limits_{x,y} \left(C_{x,y} \right)^2$	1	0,999942	1,00213
Качество корреляции $CQ = \sum\limits_{x,y} C_{x,y} \cdot S_{x,y} \Big/ \sum\limits_{x,y} C_{x,y}$	160,1201	160,1108	160,4612
Структурное содержание $SC = \sum\limits_{x,y} \left(C_{x,y} \right)^2 \Big/ \sum\limits_{x,y} \left(S_{x,y} \right)^2$	1	1,000095	0,995753

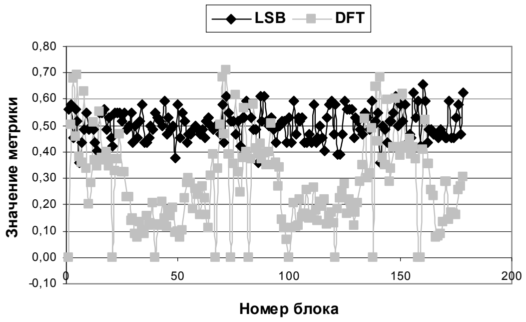


Рисунок 1 – Средняя абсолютная разность, *AD*

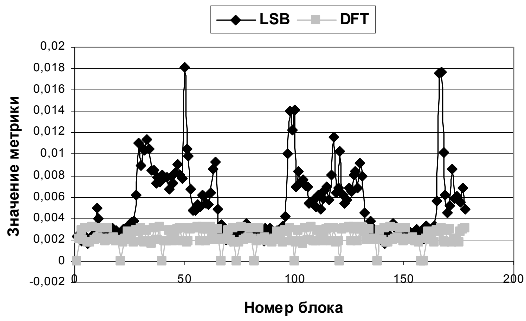


Рисунок 2 – Нормированная средняя абсолютная разность, *NAD*

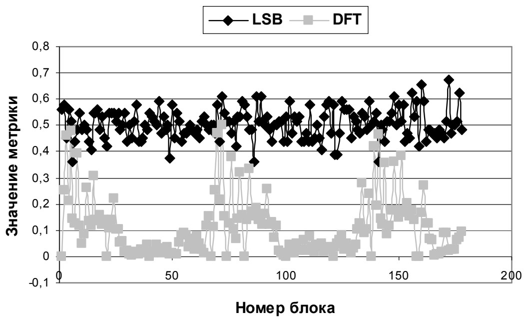


Рисунок 3 – Среднеквадратическая ошибка, *MSE*

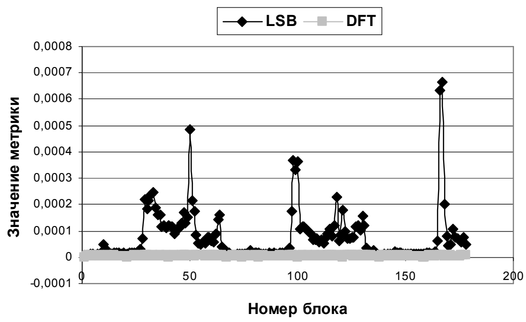


Рисунок 4 – Нормированная среднеквадратическая ошибка, *NMSE*

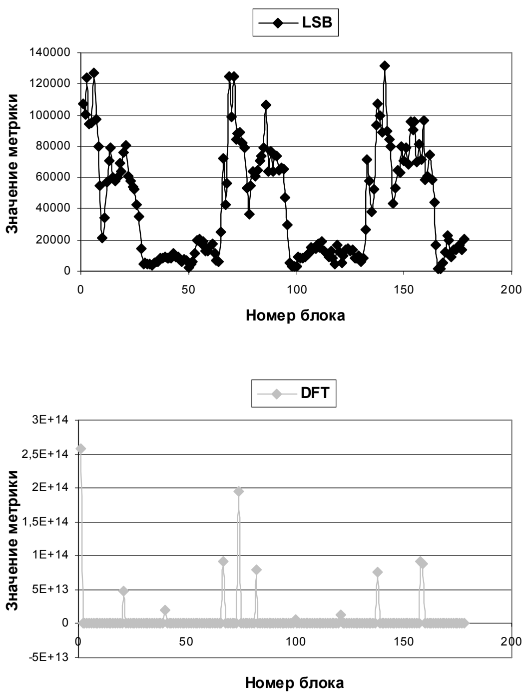


Рисунок 5 – Отношение «сигнал/шум», *SNR*

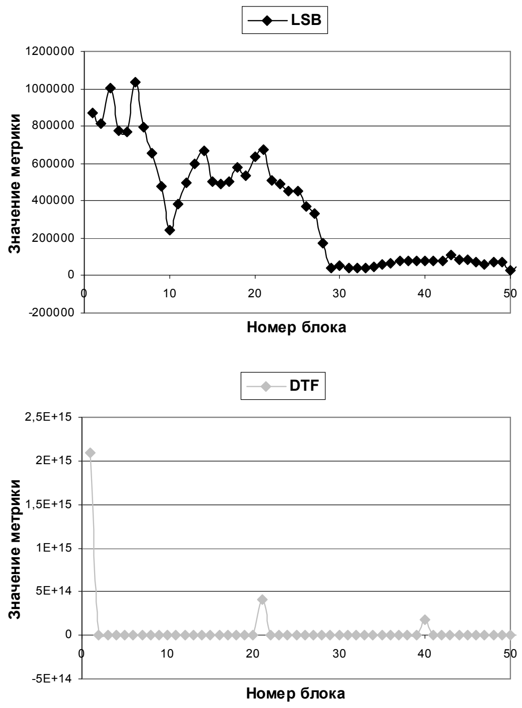


Рисунок 6 – Максимальное отношение «сигнал/шум», *PSNR*

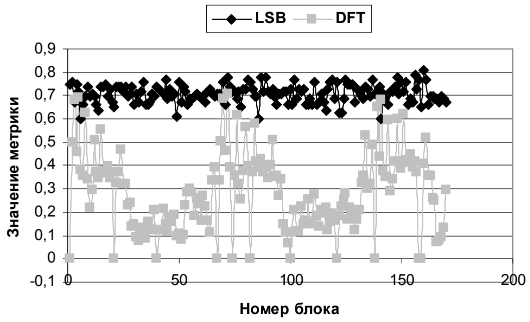


Рисунок 7 – L_2-норма

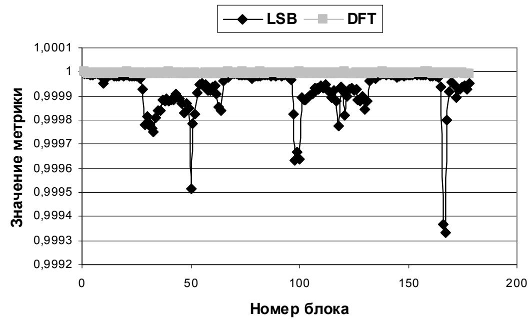


Рисунок 8 – Качество изображения, *IF*

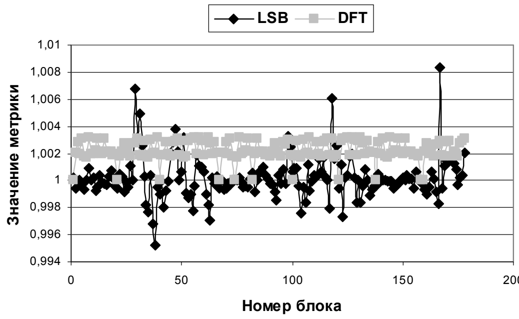


Рисунок 9 – Нормированная взаимная корреляция, *NC*

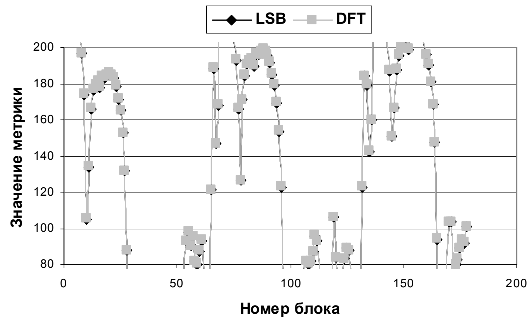


Рисунок 10 – Качество корреляции, *CQ*

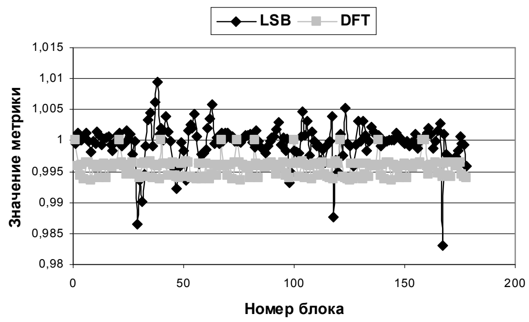


Рисунок 11 – Структурное содержание, *SC*

Результаты вычисления параметров визуального искажения в случае скрытия данных в спектральной области изображения показали, что отличие между контейнером-оригиналом и контейнером-результатом меньше, чем в случае скрытия данных методом НЗБ. Следует отметить, что в силу предъявляемых к стеганографическим системам требований, еще на стадии разработки, важно анализировать искажения, вносимые в пустой контейнер. Таким образом, разработчик сможет добиться определенного соотношения между устойчивостью встроенного сообщения к различным видам атак и размером данного сообщения.

Выводы

Любая надежная стеганографическая система представляет собой сложный комплекс, общая стойкость которого не определяется лишь только стойкостью используемого скрывающего преобразования. Большую роль для надежности всей

системы играет правильное согласование всех компонентов и точное следование всем заданным ограничениям. В противном случае любой, даже самый совершенный стеганографический метод может привести к выявлению скрываемой информации.

Совместное использование стойких криптографических алгоритмов со стеганографическим алгоритмом, реализованным на базе теоремы про свертку, позволяет достичь высокой пропускной способности создаваемого стеганоканала и сравнительно высокой стойкости против искажений в канале и возможных атак противника, с практически не изменяемым в процессе обработки контейнером.

Результаты тестирования показали эффективность предложенного способа построения криптостеганографических систем.

Объединив криптографический и стеганографический методы, можно разработать новые более стеганостойкие методы решения задач компьютерной стеганографии.

Литература

1. Перепелицын Е.Г. Нестандартные методы математической статистики и их приложение к технической диагностике и анализу изображений. – Москва: Омега-Л, 2006. – 312 с.
2. Швидченко И.В. Анализ криптостеганографических алгоритмов // Проблемы управления и информатики. – 2007. – № 4. – С. 149-155.
3. Бородавка Н.В., Задирака В.К. Стеганоалгоритмы на базе теоремы о свертке // Кибернетика и системный анализ. – 2004. – № 1. – С. 139-144.
4. Алиев А.Т., Аграновский А.В. Вопросы построения криптостеганографических систем. Модель стеганографического канала передачи данных // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 79-91.
5. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.
6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

І.В. Швідченко

Стійкі криптостеганографічні алгоритми

У статті запропоновано підхід до поліпшення стеганостійкості алгоритмів приховування інформації за рахунок спільного використання криптографічних перетворень інформації зі стеганографічними. Дано оцінку якості криптостеганографічних систем.

I.V. Shvidchenko

Stabilized Cryptosteganographic Algorithms

The approach to the improvement of algorithms' steganostability of information embedding due to the joint use of cryptographic information transformations with steganographic ones is offerred. The evaluation of cryptosteganographic systems' quality is given.

Статья поступила в редакцию 17.07.2008.